DETAILED ACTION

This office action is in response to Applicant's arguments filed on 07/18/08. Claims 1-39 are still pending in the application.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21 (2) of such treaty in the English language.

Claims 1-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Albert et al. hereinafter "Albert US PUB Number 2003/0177389.

As per claim 1, Albert teaches an apparatus for managing access to a resource over a network, comprising:

a transceiver (fig 3; client/server communication; 0072) arranged to receive a request for access to the resource from a client device; and an integrity management

component, coupled to the transceiver, that is arranged to perform actions (fig 4,423; par 0073-0074; 0077), including: providing a component to the client device (fig 4); employing the component to gather integrity information associated with the client device, wherein the integrity information is gathered at a plurality of times (par 0077-0078); forwarding the integrity information to the apparatus; applying a dynamic policy for access to the resource based, in part, on he forwarded integrity information (par 0077-0081); and if the applied policy indicates a change in an integrity of the client device, performing a response based, in part, on the applied policy (fig 4; par 0097-0099; 0078-0080).

As per claim 2, Albert teaches an apparatus of claim 1, wherein the policy is manageable through a user interface at the apparatus (par 0077-0080).

As per claim 3, Albert teaches an apparatus of claim 1, wherein the integrity information further comprises an indicator that at least one of an antivirus product is enabled on the client device, a network sniffer is enabled, a screen scraper is enabled, a cracker tool is enabled, a hacker tool is enabled, a firewall is enabled, a security application is enabled, and a client certificate is available on the client device (fig 4; par 0074-0075).

As per claim 4, Albert teaches an apparatus of claim 1, wherein the integrity information further comprises a version indicator associated with at least one of an application, a process, and an operating system (par 0072-0075).

As per claim 5, Albert teaches an apparatus of claim 1, wherein the integrity information further comprises at least one of information associated with a process currently

enabled on the client device, information associated with a sequence of system calls, and whether a predetermined file has been modified (par 0080; 0061-0063).

As per claim 6, Albert teaches an apparatus of claim 1, wherein the integrity information is gathered at a predetermined rate comprising at least one of a periodic rate, a random rate, and an aperiodic rate (par 0077-0083; 0085).

As per claim 7, Albert teaches an apparatus of claim 1, further comprising: sending a query request to the client device for selected information about the integrity of the client device (par 0072-0075).

As per claim 8, Albert teaches an apparatus of claim 1, wherein forwarding the integrity information further comprises at least one of compressing, and encrypting the integrity information (0023 and 0085).

As per claim 9, Albert teaches an apparatus of claim 1, wherein the performed response further comprises at least one of denying access to the resource, terminating a connection, and restricting access to the resource (0049, 0052, 0078, 0103, and 0105).

As per claim 10, Albert teaches an apparatus of claim 1, wherein the performed response further comprises providing a higher level of access to the resource (par 0078 and 0081).

As per claim 11, Albert teaches gathering integrity information in response to a predetermined event (par 0085).

As per claim 12, Albert teaches a method of managing access to a resource over a network, comprising: receiving a request for access to the resource from a client device (fig 3; client/server communication; 0072); receiving a first integrity information

associated with the client device (fig 4; par 0072-0075); evaluating one or more policies for access based, in part, on the first integrity information (0077-0080); receiving a second integrity information associated with the client device (fig 4; par 0074-0077); evaluating one or more policies for access based, in part, on the second integrity information (par 0072-0077); and performing a response based, in part, on a difference between the first integrity information and the second integrity information (par 0077-0081).

As per claims 13-24, they have already been discussed in claims 1-12 above, therefore, they are rejected under the same rationale.

As per claim 25, Albert teaches a system for managing access to a resource over a network, comprising: a client device configured to request access to the resource (fig 3-4); and a server (fig 3-4), coupled to the client device that is configured to perform actions, including: receiving the request for access from a client device (fig 3; client/server communication; 0072); providing a component to the client device (fig 3-4; par 0072-0075); employing the component to gather integrity information associated with the client device, wherein the integrity information is gathered at a predetermined rate (0077-0081 and 0085); receiving the integrity information at the predetermined rate from the component; applying a dynamic policy for access based, in part, on the forwarded integrity information (0077-0083 and 0085); and if the applied policy indicates a change in an integrity of the client device, performing a response based, in part, on the applied policy (par 0072-0083).

Claims 26-34 have already been discussed in the rejection of claims 1-12 and 25 above. Therefore, they are rejected under the same rationale.

As per claim 35, Albert discloses a secure socket layer (par 0065 and 0071).

As per claim 36, Albert teaches an apparatus of claim 31, further comprising logic for enabling the secure communication access through a virtual private network employing Internet Protocol Security (IPSec) (par 006, 0068 and 0071).

Claims 37-39 have already been discussed in the rejection of claims 1-12, 25 and 35-36 above. Therefore, they are rejected under the same rationale.

Response to Arguments

Applicant's arguments filed on 07/18/08 have been fully considered but they are not persuasive.

Applicant argued that Albert does not disclose "an integrity management component, ..., applying a dynamic for access to the resource", as recited in Claim 1. Examiner submits that Albert discloses the features applicant is arguing about in par 0020, 0025, 0072, 0074 and 0076. Applicant is requested to review the prior art of record for further consideration.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Frantz B. Jean whose telephone number is 571-272-3937. The examiner can normally be reached on 8:30-6:00 M-f.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan J. Flynn can be reached on 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Frantz B. Jean/
Primary Examiner, Art Unit 2454